2026-4호

AI 주도권 확보를 위한 미국의 조달 전략
: 조달 지침 및 표준 계약 조항 분석을 중심으로

주요국 AI·디지털 정책 모니터링 리포트

The LENS 2026

NIA 한국지능정보사회진흥원
NATIONAL INFORMATION SOCIETY AGENCY

목 차

AI 주도권 확보를 위한 미국의 조달 전략
- 조달 지침 및 표준 계약 조항 분석을 중심으로 -

1. 미국 AI 조달 체계 분석 배경 및 개요

● **(美 AI 조달 정책의 공백)** '26년 초 부상한 AI 기업 앤트로픽과 국방부 간 계약 이행 과정의 이견*은 주로 AI 윤리에 관한 논쟁으로 주목받았으나, 한편으로는 AI 조달 계약 체계 미비에서 비롯된 구조적 공백을 드러낸 사례[1)]

* 국방부와 앤트로픽 간 계약에서, 앤트로픽은 자율 살상 무기 및 대규모 감시 목적의 모델 사용을 거부한 반면 국방부는 모든 합법적 사용(any lawful use) 허용을 요구

- '25년 7월 국방부는 앤트로픽과 2억 달러 규모의 기타 거래(Other Transaction; OT) 계약을 체결했으며, 클로드 모델은 국방부 기밀 네트워크에 배치되어 실전 운용됨
- 기타 거래 계약은 연방조달규정(Federal Acquisition Regulation; FAR)의 적용을 받지 않아 표준화된 분쟁 해결 및 구제 절차가 부재하며, 당사자 협상에 의존하는 한계 존재
- 본 사례는 AI 공공 활용을 뒷받침하는 조달 체계의 안정성 부재가 공공-민간 간 신뢰 기반의 협력과 AI 혁신 생태계 형성을 저해할 수 있음을 보여줌

● **(미국의 사례로 본 AI 조달 과제)** 앤트로픽-국방부 사례는 AI 조달 체계의 정비가 공공 분야 AI 활용 활성화의 핵심 전제임을 시사하며, 본 보고서는 관련 정책 논의를 선도해 온 미국의 사례를 분석하여 정책적 함의 도출

- 미국 AI 조달 정책을 이해하기 위해서는 우리와 다른 제도적 기반에 대한 선행 지식이 필요함에 따라, AI 조달 체계의 작동 방식과 시기별 정책 전개 과정을 검토
- 이어 '26년 4월 기준 시행 중인 핵심 조달 지침과 표준 계약 조항을 심층 분석하고, 이를 바탕으로 AI 조달 정책에 대한 시사점 도출

[분석 대상 선정 절차]

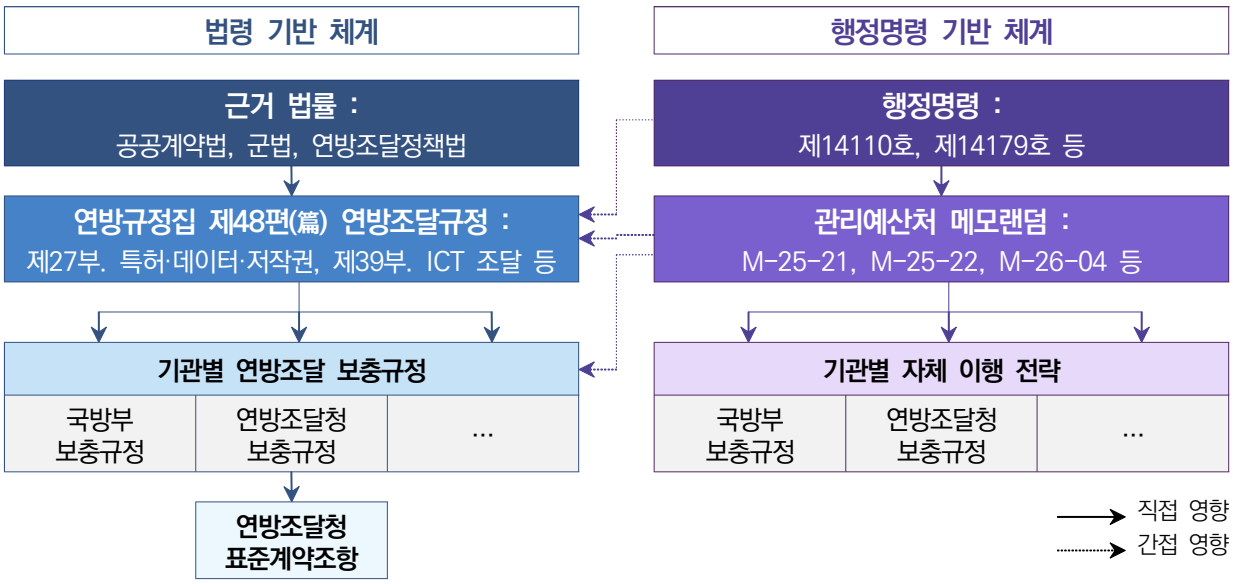
① 연방 AI 조달 관련 관리예산처(OMB)* 메모랜덤 및 연방조달청(GSA)** 규정 전수 검토
* 연방 예산 편성 및 행정기관 정책·규정 총괄 조정 기관으로, AI 조달 관련 지침 메모랜덤 발행
** 연방 정부의 물자·서비스 조달을 총괄하는 기관으로, 전 부처에 적용되는 표준 계약 조항 및 조달 규정 관리
② 철회 및 대체된 문서를 제외하고 현재 시점에서 실질적 구속력을 갖는 문서 선별
③ 최종 3개 메모랜덤(M-25-21, M-25-22, M-26-04)과 표준 계약 조항 초안(GSAR 552.239-7001) 선정

2. 미국 AI 조달의 운영 구조

● **(AI 조달 체계)** 미국 연방 AI 조달은 의회 입법에 근거한 법령 기반 체계와 대통령 행정명령에 근거한 행정명령 기반 체계가 병행하여 작동하는 구조로 운영됨

- 법령 기반 체계는 의회 입법을 근거로 하는 연방조달규정 및 부처별 보충규정으로 구성되며, 정권 교체와 무관하게 항구적으로 적용됨
- 행정명령 기반 체계는 대통령 행정명령에 따라 관리예산처가 발행하는 메모랜덤으로 구성되며, 정권 교체 시 기존 지침이 철폐·대체될 수 있음

[미국 연방 AI 조달 체계 개관]



● **(법령 기반 체계)** 「공공계약법」, 「군법」, 「연방조달정책법」*을 근거로 하며, 이를 구체적인 조달 절차로 규정한 연방조달규정을 전 연방기관에 적용

* 각각 41 U.S.C.(Federal Property and Administrative Services Act), 10 U.S.C.(Armed Services Procurement Act), Office of Federal Procurement Policy Act(OFPP Act)

- 연방조달규정은 미국 행정규칙 모음집인 연방행정규정(Code of Federal Regulations; CFR)에서 정부 조달 규정을 별도로 묶어 놓은 '제48편'에 해당하며, '제27부. 특허·데이터·저작권'과 '제39부. ICT 조달'이 핵심 근거 조항으로 기능
- 각 연방기관은 연방조달규정을 기반으로 소관 조달에 특화된 보충규정을 두며, 국방부 보충규정(Defense Federal Acquisition Regulation Supplement; DFARS)과 연방조달청 보충규정(General Services Administration Acquisition Regulation; GSAR) 등이 이에 해당
- 전 연방기관은 연방조달청이 공급업체와 사전 협상한 계약을 통해 서비스를 구매할 수 있으며, GSAR 552.239-7001은 이 계약에 적용되는 AI 조달 표준 계약 조항

● **(행정명령 기반 체계)** 대통령 행정명령이 관리예산처에 이행 지침 발행을 지시하고, 관리예산처가 메모랜덤 형식으로 전 연방기관에 하달하는 구조

- 현행('26.4월 기준) 지침은 AI 거버넌스(M-25-21), 조달 실행(M-25-22), 대규모언어모델(LLM) 편향 방지(M-26-04) 등 세 개의 메모랜덤으로 구성되며, 각 연방기관은 메모랜덤에 따라 기관별 AI 정책과 절차를 자체적으로 수립·이행
- 행정명령과 메모랜덤의 내용은 연방조달규정 개정 및 표준 계약 조항(GSAR 552.239-7001) 형태로 법령 기반 체계에 반영

3. 미국 AI 조달 정책의 전개

● **(정책 전개)** 미국 연방 AI 조달 정책은 국가 차원의 AI 정책 체계가 마련되기 시작하던 '20년을 기점으로 본격화되어, 행정부 교체에 따라 방향 전환을 거치며 현재 체계로 발전

- AI 기술의 빠른 변화에 따라 행정명령 기반 정책 추진이 주를 이루며, 정권 교체 시 조달 원칙과 요건이 전면 재편되는 특성을 보임

● **(기반 조성기 : '19~'20)** 연방정부가 AI를 조달 대상 기술로 공식 인식하고, AI 조달에 적용할 공통 원칙과 제도적 기반을 처음 구축한 시기

- 행정명령을 통해 AI 조달에 전 단계에 적용되는 정부 차원의 공통 원칙 최초 제시
- 관리예산처 지침이 연방 AI 조달 정책의 기준으로 자리 잡으며 정책 체계 형성

● **(리스크 관리기 : '21~'24)** AI 조달 계약에 구속력 있는 요건을 도입하고, 권리 및 안전에 영향을 미치는 AI를 중심으로 계약 요건을 단계적으로 세분화·강화

- 공급업체 검증, 데이터 권리 보장, 사고 보고 등 계약 의무 요건을 법·지침으로 구체화
- 권리 및 안전에 영향을 미치는 AI 등 위험 수준이 높은 분야의 조달 규정 세분화
- 관리예산처 메모랜덤을 통해 최초로 연방 차원의 AI 조달 규정 체계 형성

● **(혁신 가속·규제 철폐기 : '25~현재)** 위험 관리 중심 조달 체계를 혁신 촉진, 효율성 향상, 산업 경쟁력 제고를 중심으로 전면 재편

- 기존 조달 지침을 폐지·대체하고 상용화된 미국산 AI 우선 조달 원칙 도입
- 오픈 API, 데이터 이식성, 복수 모델 선택 등 시장 경쟁 촉진형 계약 구조 도입
- 조달 지침을 표준 계약 조항으로 명문화하려는 시도를 본격화하며 제도적 구속력 강화

[미국 연방정부 AI 조달 정책 연혁]

※ 다음의 표에서 색으로 강조 표시된 정책은 본 보고서의 분석 대상에 해당함

시기	유형	기관	명칭	조달 관련 주요 내용	현재 상태
■ 기반 조성기 : 트럼프 1기 행정부('19~'20)					
'20.12	행정명령	백악관	제13960호 신뢰할 수 있는 AI의 연방정부 사용 촉진[2]	▪ AI 설계, 개발, 조달, 활용 전 단계에 걸친 9대 원칙 적용 명시	유효
'20.12	법률	의회	정부AI법 2020[3]	▪ 연방조달청의 AI전문역량센터 설치에 대한 근거 부여 및 AI 조달 자문 기능 명시 ▪ 관리예산처의 지침을 연방 AI 조달 정책의 준거 기준으로 명시	유효
■ 리스크 관리기 : 바이든 행정부('21~'24)					
'22.10	법률	의회	조달인력의 AI 역량강화법[4]	▪ 관리예산처와 연방조달청의 협력으로 연방 조달 인력의 AI 교육 프로그램 수립·운영	유효
'22.12	법률	의회	미국AI진흥법[5]	▪ AI 조달 계약 요건 법제화 ▪ 조달 간소화 제도 적용이 가능한 혁신적 상용 AI 제품 계약 금액 상향	유효
'23.10	행정명령	백악관	제14110호 안전하고 신뢰할 수 있는 AI 개발 및 사용[6]	▪ 관리예산처에 AI 조달 계약 요건 정비 지시 ▪ 연방조달청에 연방 AI 조달 체계 마련 지시 ▪ 연방조달규정 개정 검토 지시	폐지
'24.03	메모랜덤	OMB	M-24-10 AI의 기관 활용을 위한 거버넌스, 혁신, 위험 관리 촉진[7]	▪ 공급업체 주장 독립적 검증, 공급업체 락인 방지, 정부 데이터 권리 확보, 생성형 AI 및 바이오메트릭 AI 조달 시 추가 요건 권고	폐지
'24.04	지침	GSA	생성형 AI·특수 컴퓨팅 인프라 조달 가이드[8]	▪ 조달 목적에 맞는 계약 방식 선택 안내 ▪ 데이터 보호 및 비용 관리 권고	상위근거 (행정명령 제14110호) 폐지
'24.09	메모랜덤	OMB	M-24-18 정부의 책임 있는 AI 조달 촉진[9]	▪ 권리 및 안전에 영향을 미치는 AI 계약 시 사고 보고, 데이터 관리, 테스트 요건 의무화 ▪ 공급업체 락인 방지 및 정부 데이터 소유권 계약서 명시	폐지
■ 혁신 가속·규제 철폐기 : 트럼프 2기 행정부('25~현재)					
'25.01	행정명령	백악관	제14179호 미국의 AI 주도에 대한 장벽 제거[10]	▪ 행정명령 제14110호 폐지 ▪ 관리예산처에 기존의 AI 거버넌스(M-24-10) 및 조달 지침(M-24-18) 개정 지시	유효
'25.04	메모랜덤	OMB	M-25-21 혁신, 거버넌스, 공공 신뢰를 통한 연방정부 AI 활용 가속화[11]	▪ M-24-10 대체 ▪ 고영향 AI 조달 시 위험 평가, 인간 감독, 지속적 성과 모니터링 요건 포함 의무화	유효

[미국 연방정부 AI 조달 정책 연혁(계속)]

시기	유형	기관	명칭	조달 관련 주요 내용	현재 상태
'25.04	메모랜덤	OMB	M-25-22 정부의 효율적인 AI 조달 추진[12]	▪ M-24-18 대체 ▪ 상용 AI 및 미국산 AI 우선 조달, 오픈 API 의무화, 데이터 이식성 및 상호운용성 확보, 정부 데이터의 상용 모델 훈련 금지 등	유효
'25.07	전략	백악관	AI 실행계획[13]	▪ 복수의 AI 모델을 선택·조달할 수 있는 통합 조달 플랫폼 구축 지시 ▪ 조달 LLM에 이념 중립, 객관성 요건 적용	유효
'25.07	행정명령	백악관	제14319호 연방정부에서의 특정 성향 AI 금지[14]	▪ 연방 LLM 조달 계약에 편향 없는 AI 원칙(진실 추구, 이념 중립) 의무화 ▪ 관리예산처에 이행 지침 지시 마련 지시	유효
'25.12	메모랜덤	OMB	M-26-04 편향 없는 AI 원칙을 통한 AI에 대한 공공 신뢰 제고[15]	▪ LLM 조달 계약 시 공급업체의 모델 편향 검증 문서 제출 의무화	유효
'26.03	표준 계약 조항	GSA	GSAR 552.239-7001 AI 시스템의 기본적 안전 보호조치[16]	▪ 미국산 AI 우선 조달, 외산 AI 조달 금지, AI 산출물 정부 귀속, 표준 API 및 데이터 형식 의무화, 사이버 사고 72시간 내 보고	최종 문안 검토 중 ('26.4월 기준)

4. 현행 AI 조달 지침의 주요 내용

❶ M-25-21 혁신, 거버넌스, 공공 신뢰를 통한 연방정부 AI 활용 가속화

Accelerating Federal Use of AI through Innovation, Governance, and Public Trust

● **(수립 목적)** 바이든 정부에서 수립한 M-24-10을 폐지·대체하여 혁신 촉진, 거버넌스 강화, 공공 신뢰 촉진의 세 축을 중심으로 연방 AI 활용 가속화를 위한 기관 이행 지침 제시

- **혁신 촉진** : 각 기관이 AI 전략 수립, 데이터·코드 공유, 미국산 AI 우선 조달, 성과 추적, 인력 역량 강화에 관한 구체적 조치를 이행할 것을 지시

※ **주요 조치** : 기관별 AI 전략 수립·공개, 자체 개발·조달한 AI 코드·모델 등 자산 공유, 미국산 AI 우선 조달, AI 조달 성과 지속적 평가, 공공분야 기존 인력 역량 강화 및 AI 인재 채용·유지

- **거버넌스 강화** : 기관 최고AI책임자(Chief AI Officer)* 지정 및 AI 거버넌스 위원회(Agency AI Governance Board)** 구성, 범정부 최고AI책임자 협의체(Chief AI Officer Council)*** 운영

* 기관 내 AI 혁신, 도입, 거버넌스를 총괄하고 고영향 AI 판정, 모니터링, 운용 승인 절차 수립 책임

** IT, 법무, 프라이버시, 시민권 등 핵심 부서가 참여하여 기관 내 AI 활용에 관한 사안을 조율 및 감독

*** 관리예산처 주재 하에 각 기관 최고AI책임자가 참여하여 범정부 AI 개발·활용 조율 및 모범사례 공유

- **공공 신뢰 촉진** : 고영향 AI의 판정 및 결과 공개, 7대 최소 위험 관리 기준 의무화

● **(AI 조달 지침)** 고영향 AI 최소 위험 관리 기준 준수를 지원하기 위한 AI 조달 방향을 제시하며, 데이터 가치 보호, 성과 추적, 경쟁 촉진을 조달의 핵심 요소로 규정

- **데이터 가치 보호** : 정부 데이터 및 개선 결과물에 대한 권리를 확보하고, 기관의 명시적 허가 없이 공급업체의 상업용 AI 훈련·기능 개선에 활용되는 것을 계약상 차단
- **성과 추적** : 조달한 AI의 역량·한계 및 훈련 데이터 출처를 문서화하고, 실제 운영 조건에서의 성과 테스트, 과적합 점검, 사후 모니터링 체계를 계약에 반영
- **경쟁 촉진** : 상호운용성 있는 AI 제품·서비스를 우대하는 경쟁 조달 관행을 채택하여 연방 AI 시장의 건전한 경쟁 생태계 유지

참 고 고영향 AI 분야 및 판정 기준

● **(고영향 AI)** 기존 지침(M-24-10)의 ▲안전 및 ▲권리에 영향을 미치는 AI 이중 분류를 고영향 AI 단일 개념으로 통합하고, 15개 범주에 해당하는 AI를 고영향 AI로 추정

1 핵심 인프라 및 정부 시설의 안전 기능, 교통 통제 시스템 등	2 로봇, 차량, 장비 등 물리적 이동에 따른 신체 위해 가능 시스템	3 실세계에서 인체 피해를 유발할 수 있는 공격·방어 수단
4 위험 화학물질 및 생물학적 물질의 운반·설계·사용	5 안전 위험이 있는 장비, 시스템, 공공 인프라의 설계·구축·테스트	6 의료기기, 환자 진단, 치료, 공공보험 내 의료 자원 배분 등 의료 맥락
7 정부 시설 접근 통제 및 보안	8 수출 통제, 무역 제재, 투자 제한 등의 집행	9 보호된 표현의 차단, 삭제, 은폐, 확산 제한
10 법집행 맥락에서의 위험 평가, 용의자 식별, 범죄 예측, 생체인식, 위치 추적 등	11 외국인 출입국, 망명, 구금, 여행 허가 관련 위험 평가	12 공개 공간에서의 일대다 생체인식
13 연방 서비스, 급여, 대출, 공공주택 신청 및 자격 심사·부정 탐지	14 채용, 해고, 성과관리, 보직 변경 등 연방 고용 조건 결정	15 법적 구속력이 있거나 기관의 결정에 직접 영향을 미치는 언어 번역

● **(판정 기준)** AI 산출물이 다음의 6개 영역에서 개인·기관에 법적·실질적·구속적·중대한 영향을 미치는 결정이나 행동의 주요 근거로 기능하는 경우 고영향 AI로 판정

1 개인·기관의 시민권, 시민적 자유, 프라이버시	2 교육, 주거, 보험, 신용, 고용 등 각종 프로그램 접근	3 핵심 정부 자원 및 서비스에 대한 접근
4 인간의 건강 및 안전	5 핵심 인프라 및 공공 안전	6 고가 자산, 민감·기밀 정보 등 전략적 자원

※ 출처 : M-25-21 혁신, 거버넌스, 공공 신뢰를 통한 연방정부 AI 활용 가속화

❷ M-25-22 정부의 효율적인 AI 조달 추진
Driving Efficient Acquisition of Artificial Intelligence in Government

● **(수립 목적)** 바이든 정부에서 수립한 M-24-18을 폐지·대체하여 현행 연방 AI 조달 실행 지침으로, EO 14179 및 M-25-21의 조달 부문 이행 문서

- 메모랜덤을 관통하는 3대 기조로 ① 미국 AI 시장 경쟁력 확보, ② 납세자 자금 보호를 위한 성과 추적 및 위험 관리, ③ 범기능 협력에 기반한 효과적 조달 제시
- 기관이 기본적으로 지켜야 할 요건과 조달 생애주기 6단계 구조로 전면 재편하여 조달 실무자 중심의 단계별 참조 체계 구축

● **(의무 요건)** 조달 생애주기 가이드에 앞서 기관이 갖추어야 할 제도적 기반 요건 규정

- **내부 정책 정비** : AI 조달 관련 정책과 절차를 M-25-21 및 행정명령 제14179호에 부합하도록 갱신하고, 생성형 AI 허용 기준과 안전장치를 담은 별도 정책 수립
- **미국산 AI 우선 조달** : 미국에서 개발·생산된 AI 제품 및 서비스의 활용을 극대화하는 'Buy America' 원칙 반영
- **데이터·지식재산권 보호** : 정부와 공급업체 간 권리를 명확히 하는 기관 표준 절차를 수립하고 비공개 정부 데이터와 산출물을 공급업체 AI 훈련에 활용하는 행위를 영구 금지
- **프라이버시 보호** : 개인식별정보를 처리하는 AI 조달 시 개인정보보호 고위책임자(Senior Agency Official for Privacy)의 사전·지속적 참여 보장

● **(생애주기별 가이드)** 요건 식별부터 계약 종료까지 AI 조달 전 과정을 6단계로 구분하여 단계별 핵심 활동과 필수 이행 과제 제시

[AI 조달 생애주기 단계별 이행 과제]

1 요건 식별	2 시장 조사 및 기획
▪ 범기능(cross-functional) 팀 구성 - 조달의 복잡성과 위험에 맞춰 자원 배분 - 연방정부 AI 활용 원칙 관련 위험 식별 ▪ 고영향 AI 사용 사례 해당 여부 판정 - 예측가능한 사용 사례 기반으로 판정 실시 - 시장 조사 핵심 질문 도출 기준으로 활용	▪ 광범위한 시장 조사 - 부처 간 지식 공유 및 조달 플랫폼 적극 활용 - 신규 진입 업체 역량까지 폭넓게 탐색 ▪ 제품 시연 - 실제 운영 환경 시나리오에서 시연·테스트 실시 - 공급업체 역량·한계 및 장기 비용 효율성 점검 ▪ 성과 기반 조달 기법 활용 - 목표기술서(SOO) 및 성과업무기술서(PWS) 활용 - 품질보증감시계획(QASP) 수립 - 성과 기반 계약 인센티브 설계

[AI 조달 생애주기 단계별 이행 과제(계속)]

3 공모서 작성	4 낙찰자 선정
▪ AI 활용 투명성 요건 공시 - 고영향 활용 사례 해당 여부 입찰공고에 명시 - 공급업체에 투명성 및 문서화 요건 사전 고지 ▪ 공급업체 종속 방지 조항 반영 - 기술 이전 및 데이터와 모델 이식성 요건 포함 - 라이선스 조건 및 가격 투명성 확보 ▪ 지식재산권 및 정부 데이터 활용 조항 포함 - 旣 수립한 지식재산권 및 데이터 소유권 표준 절차 반영	▪ 테스트 및 평가 실시 - 제안된 솔루션의 역량 및 한계 확인 - 기관 네트워크 내 전용 테스트 환경 구축 검토 ▪ 기회 및 위험 재검토 - 선정 전 AI 관련 위험 재평가 - M-25-21 준수 요건 관련 애로 사항 사전 점검 ▪ 계약 필수 조항* 포함 * 지식재산권 및 정부 데이터 활용, 프라이버시 보호, 공급업체 종속 방지. M-25-21 준수 요건, 테스트 및 모니터링 권한, 공급업체 성과 요건, 신기능 사전 통보
5 계약 관리	**6 계약 종료**
▪ 운영 허가 취득 - 정보시스템 배포 전 기관 담당자 허가 필수 ▪ 계약 감독 수행 - 프라이버시·시민권 관련 신규 위험 식별·완화 ▪ 성과 및 비용 타당성 평가 - 효과성, 효율성, 운영 비용 정기 평가 - 이해관계자 피드백 수렴 및 반영 ▪ 사용 중단 기준 설정 - 비용, 수요, 성과 변화 시 재검토 기준 마련	▪ 공급업체 종속 방지 - 데이터 및 파생 산출물 권리 이행 확인 - 데이터 형식 및 접근권 상호 확인 - 데이터 이전 계획 수립

● **(조달 인프라 구축)** 행정부 내부 전용 모범사례 공유 저장소를 구축하고, 생체인식, 특수 컴퓨팅 인프라, 생성형 AI 등 AI 유형별 특화 플레이북 개발

❸ M-26-04 편향 없는 AI 원칙을 통한 AI에 대한 공공 신뢰 제고
Increasing Public Trust in Artificial Intelligence through Unbiased AI Principles

● **(수립 목적)** 행정명령 제14319호의 이행 지침으로, 연방정부가 조달하는 LLM이 편향 없는 AI 원칙(진실 추구, 이념적 중립성)을 준수하도록 규정하여 M-25-22를 보완

- **진실 추구**(Truth-seeking) : LLM은 사실 정보·분석 요청에 진실하게 응답하고, 역사적 정확성, 과학적 탐구, 객관성을 우선시하며 불확실성을 인정

- **이념적 중립성**(Ideological Neutrality) : LLM은 특정한 이념적 신조에 편향되지 않는 중립적이고 비당파적 도구로 기능

● **(적용 대상)** 메모랜덤 발행일('25.12.11) 이후 연방기관이 조달하는 모든 LLM에 배포·수정·활용 방식과 무관하게 적용되며, 국가안보시스템은 원칙적으로 제외

- 신규 계약에는 즉시, 기존 계약에는 계약 연장 전까지 원칙 준수 요건을 반영하며, 각 기관은 조달 정책·절차를 업데이트하고 원칙을 위반한 산출물에 대한 내부 보고 절차 마련

● **(계약 요건)** LLM 조달 시 공급업체의 역할에 맞게 편향 없는 AI 원칙 준수 확인에 필요한 정보를 요청하되, 모델 가중치 등 민감 기술 데이터 공개 강요는 지양

[편향 없는 AI 원칙 준수를 위한 LLM 조달 계약 요건 체계]

구분	내용
최소 기준 (Minimum Threshold)	모든 LLM 조달 시 필수 요청 - 제품의 사용의 적절성과 부적절성을 구분하여 규정하는 정책 문서 - 모델, 시스템, 데이터에 관한 핵심 정보를 포함한 카드 - 튜토리얼 등 최종 사용자의 LLM 활용 자원 수단 - 최종 사용자 피드백 메커니즘
강화 기준 (Enhanced Threshold)	기관의 계획된 활용 목적에 따라 추가 요청 - 모델의 사전 및 사후 훈련 활동 - 편향 평가 결과 및 방법론, 벤치마크 점수 - 거버넌스, 평가, 출처 확인 등 기업 차원의 통제 도구 - 공급업체가 직접 개발자가 아닌 경우 산출물 수정을 위한 통제 수단 공시
중대성 요건 (Materiality)	상기 요건을 계약 자격 및 지급의 실질적 조건으로 명시하여, 공급업체의 시정 조치 거부 시 계약 불이행 해지 근거로 활용

❹ GSAR 552.239-7001 표준 계약 조항 - AI 시스템의 기본적 안전 보호조치
Basic Safeguarding of Artificial Intelligence Systems

● **(제안 목적)** 연방조달청이 작성한 AI 시스템 표준 계약 조항 초안으로, M-25-21, M-25-22, M-26-04의 정책 의도를 법적 구속력 있는 계약 의무로 전환

- 계약관은 AI 기능이 포함된 모든 공모서 및 계약에 본 조항을 필수 삽입해야 하며, 공급업체 또는 서비스 제공자의 상업적 약관·정책과 충돌 시 본 조항이 우선 적용

- 직접 계약 당사자인 공급업체는 AI 시스템을 실질적으로 운용하는 서비스 제공자(Service Provider)*의 조항 준수에 대해서도 책임을 부담

* 계약의 당사자는 아니나, AI 시스템을 직접 또는 간접적으로 제공, 운영, 라이선스하는 주체

● **(조항 구성)** 본 조항은 정부, 공급업체, 서비스 제공자 간 권리·의무를 ① 데이터 및 지식재산권, ② 이행·보고·문서화, ③ 데이터 이식성 및 변경 관리, ④ 성과 평가 및 불이행 등 4개 영역으로 규율

[조항별·주체별 의무]

조항	정부	공급업체	서비스 제공자
■ 데이터 및 지식재산권			
정부 데이터 소유권 : 데이터 입출력 및 커스텀 개발물에 대한 완전한 소유권 보유, 지식재산권 생성 즉시 자동 양도	● 소유권 보유	● 제한적 사용 허용	● 공급업체와 동일 계약 적용
정부 이용 허가 : 정부에 AI 시스템 이용 철회 불가·무상 비독점 라이선스 부여, AI가 출력·분석을 거부할 수 없음	● 라이선스 취득	● 라이선스 부여 의무	-
정부 데이터 금지 사용 : 공급업체 AI 모델 훈련 및 파인튜닝에 활용 금지, 광고·마케팅 등에 활용 금지, 계약에서 허용된 범위·기간 초과 보유·접근 금지	-	● 준수 의무	● 동일 적용
데이터 보안 및 처리 : 인간의 정부 데이터 직접 열람 제한(eyes off) 원칙 적용, 데이터 현지화·논리적 분리 의무, 계약 종료 시 완전 삭제 및 인증	● 접근 로그 열람권	● 이행 의무	● 동일 적용
■ 이행·보고·문서화			
미국산 AI 사용 의무 : 미국에서 개발·생산된 AI 시스템만 허용, 非 미국 주체가 제조·통제하는 외산 AI 전면 금지	-	● 준수·공시 의무	● 동일 적용
인간 감독 및 추적 가능성 : 중간 처리(추론·검색·에이전트) 단계 요약 제공, 모델 선택 근거 및 참고 자료 출처 명시 포함	● 감독 수단 활용	● 도구 제공 의무	-
사고 보고 : 72시간 내 사이버보안·인프라보안청(CISA) 사고 보고 양식 제출 및 계약관 통보, 관련 로그·포렌식·아티팩트 90일 이상 보존	● 통보 수령·조사	● 보고 의무	● 보존 의무
문서화 : 정부 요청 시 국립표준기술연구소 「AI 위험관리 프레임워크」 및 편향 없는 AI 원칙 준수 증빙 문서, 시스템 카드 등 제출	● 요청, 기밀 유지	● 제출 의무	-
■ 데이터 이식성 및 변경 관리			
데이터 이식성 및 상호운용성 : JSON·XML 등 개방형 표준 API 및 데이터 형식 사용 의무화, 공급업체 종속 금지	● 내보내기 권리	● 도구 제공 의무	● 독점 포맷 금지
변경 관리 : 주요 버전 변경 30일 및 경미한 버전 변경 15일 사전 평가 기간 제공, 편향 증가 및 안전장치 약화 변경은 7일 내 통보	● 사전 평가권	● 사전 통보 의무	● 서비스 교체 30일 전 통보
■ 성과 평가 및 불이행			
편향 없는 AI 원칙 : 진실 추구·이념적 중립성 준수, 다양성·형평성·포용성 등 이념적 신조 산출 금지, 지속적 개선 프로세스 운영	-	● 상업적 노력 의무	-
정부 평가 권한 및 불이행 : 자체 벤치마크를 통해 수시로 자동화 평가 실시 가능, 원칙 위반 시 사용 중단·해지 권리 보유	● 평가, 중단, 해지권	● 해지 비용 부담	-

5. 미국 AI 조달 정책 특징 분석 및 시사점

5-1 미국 AI 조달 정책 특징

[미국 AI 조달 정책은 공공 부문 AI 활용의 주요 쟁점에 다음 다섯 가지 방식으로 대응]

- **(정부 데이터 소유권 보호)** 정부 데이터가 공급업체의 상업용 모델 개선에 무상으로 기여하는 구조에 대응하기 위해, 데이터의 상업적 활용 금지와 처리 방식을 규율하는 방식 모색
  - M-25-22[AI 조달 지침]는 비공개 기관 데이터·산출물의 상업용 AI 훈련·파인튜닝 활용을 계약상 영구 금지하며, GSAR 552.239-7001[AI 표준 계약 조항]은 이 원칙을 계약 조항 수준에서 구체화
  - 상업적 활용 차단을 뒷받침하기 위해 공급업체의 정부 데이터 열람 원칙적 제한, 데이터 현지화, 계약 종료 시 완전 삭제를 표준 계약 의무로 규정
- **(공급업체 의존 구조 방지)** AI 도입 후 특정 시스템 종속으로 공급업체 교체 비용이 급증하는 문제에 대응하여, 미국은 조달 초기 단계부터 교체 가능성을 확보하는 방식을 채택
  - '**AI 조달 지침**[M-25-22]'은 공모서 작성 단계에서부터 데이터·모델 이식성, 기술 이전 조건, 라이선스 가격 투명성을 반영하도록 규정하여, 조달 초기부터 공급업체 교체 여건 확보
  - '**AI 표준 계약 조항**[GSAR 552.239-7001]'은 '**AI 조달 지침**[M-25-22]'의 원칙을 기술 표준 수준에서 구체화하여, 개방형 API 및 데이터 형식 사용 의무화와 독점 기술 사용 금지를 계약 조항으로 명문화
- **(고영향 AI의 체계적 판정)** AI 전반을 규율하는 법률 제정을 지양하는 기조 하에, AI 시스템의 영향력에 기반한 판정·관리 체계 설계를 조달 정책의 핵심 과제로 설정
  - '**AI 거버넌스 지침**[M-25-21]'은 기존 지침에서 ▲안전에 영향을 미치는 AI와 ▲권리에 영향을 미치는 AI로 이원화되어 있던 분류 체계를 고영향 AI로 통합하여 판정·관리의 일관성 확보
  - '**AI 조달 지침**[M-25-22]'은 조달 요건 식별 단계에서 고영향 AI 여부를 초기 판정하도록 규정하여, 해당 판정 결과가 시장 조사, 공모서 작성, 계약 조건 전반의 기준이 되도록 설계
- **(AI 결정에 대한 책임 소재 명확화)** AI가 정부 결정에 관여할 때 발생하는 다주체 간 책임 소재 문제에 대응하여, 기관 내부 거버넌스와 계약 당사자 간 책임 관계를 동시에 규정
  - '**AI 거버넌스 지침**[M-25-21]'은 기관 최고AI책임자에게 고영향 AI의 판정·모니터링 책임을 부여하고, AI 영향 평가서에 위험 수용 서명을 의무화하여 책임 소재를 문서로 확정

- ‘AI 표준 계약 조항GSAR 552.239-7001’은 계약 당사자인 공급업체가 AI 시스템을 실제 운용하는 서비스 제공자의 조항 준수에 대해서도 책임을 부담하도록 규정하여, 책임 공백 차단

● **(공급업체 주장에 대한 신뢰 검증)** 공급업체가 공개하는 정보에 의존할 수밖에 없는 정보 비대칭에 대응해, 공급업체의 투명성 의무 및 정부의 독립 평가 권리를 계약으로 명문화

- ‘LLM 편향 방지 지침M-26-04’은 LLM 조달 시 모델 카드, 편향 평가 결과 등 투명성 문서를 의무화하며, ‘AI 표준 계약 조항GSAR 552.239-7001’은 정부의 자동화 평가 권한과 중대 변경 시 사전 통보 의무 명시

5-2 시사점

[미국 AI 조달 정책 분석 결과, 공공 AI 조달 정비를 위한 시사점은 다음 세 가지로 수렴]

● **(분쟁 다발 영역의 표준 계약화)** 미국은 계약 당사자 간 갈등이 발생하기 쉬운 영역을 표준 계약 조항으로 명문화하여, 기관별 계약 작성 시 참조할 수 있는 공통 기준 제공

- 데이터 소유권, 공급업체 의존 구조 방지, 미국산 AI 사용 의무, 사고 보고 기한 등 정부-공급업체 간 이해관계가 충돌하기 쉬운 쟁점을 GSAR의 조항으로 문안 표준화

➢ 학습 데이터 권리 관계, 생성형 AI 산출물 귀속, 외산 AI 도입 시 검증 의무 등 조달 현장에서 반복적으로 제기되는 쟁점을 표준 계약 조항 수준에서 명문화할 필요

● **(성능 기반 검증 구조)** 미국은 문서 형식의 준수 심사를 넘어, 기관이 실제 운영 환경에서 AI 산출물과 성과를 직접 검증할 수 있는 권한 부여

- 조달 초기 시장 조사 단계에서 실제 운영 환경 시나리오 기반의 제품 시연을 의무화하고, 계약 이후에도 정부의 자동화 평가 권한과 중대 변경 시 사전 통보 의무 규정

➢ 문서 중심의 평가 방식이 AI 산출물의 실제 품질을 검증하기 어렵다는 한계를 고려하여 계약 전 개념 검증(POC) 절차 도입, 산출물에 대한 평가 방식의 다원화, 계약 이후 지속적 성과 평가 체계 마련을 검토할 필요

● **(의사결정의 전문성·유연성)** 미국은 AI 기술의 복잡성과 불확실성에 대응하기 위해 조달 의사결정 구조를 전문화·유연화하는 방향으로 정비

- 기관별 전담 책임자 지정을 의무화하여 AI 조달의 전문성을 제도적으로 확보하고, 조달 생애주기 전 단계에서 요건 재평가와 조건 조정이 가능한 방식으로 설계

➢ 절차적 공정성 중심의 조달 방식이 AI 전환기의 빠른 기술 변화와 다양한 도입 방식을 수용하기 어려운 한계를 고려하여, 간소화된 계약 경로의 확대 적용과 조달 주체의 AI 전문성 강화 병행

□ 함께 보면 좋은 정책 자료

자료명	AI 플레이북 Artificial Intelligence Playbook[17]				
국가/기관	영국	자료 유형	지침·가이드라인	발표 일자	2025. 2. 10.

● 영국 정부는 공공부문의 AI 도입·활용 전반에 대한 통합 지침으로서 'AI 플레이북' 개발

- AI 플레이북은 영국이 '24년 발표한 생성형 AI 프레임워크(Generative AI Framework for HMG)를 확장·개편한 것으로, AI 도입 全 과정을 하나의 정책 체계로 통합하며 공공부문에서 AI를 안전하고 효과적으로 구매·운영하기 위한 프레임워크 제시
- AI 플레이북은 ▲AI 정의와 한계 이해, ▲법·윤리 준수, ▲보안, ▲인간 통제 유지, ▲전 생애주기 관리, ▲적합한 도구 선택, ▲개방성과 협업, ▲초기부터 조달 담당 동료와 협업, ▲역량·전문성 확보, ▲거버넌스·보증 체계 구축 등 10가지 핵심 원칙 제시
- AI 플레이북은 AI 도입에 앞서 해결하고자 하는 문제에 AI가 적합한 도구인지를 판단하도록 하고, 프로젝트 초기 단계부터 조달 담당 인력과의 협업, 공급업체 종속 방지, 데이터 윤리, 보안 등 요구사항의 사전 정의와 조달 과정 공정성·투명성 확보 권고

자료명	AI 표준 계약 조항 Model Contractual Clauses for AI[18]				
국가/기관	EU	자료 유형	지침·가이드라인	발표 일자	2025. 3. 5.

● EU의 AI 공공조달 실무공동체(Community of Practice on Public Procurement of AI)는 「AI법(AI Act)」의 요건을 조달 계약에 반영할 수 있도록 표준 계약 조항 개발

- AI 공공조달 실무공동체는 '23년 9월 표준 계약 조항의 초판을 발표한 후, 「AI법」 공식 채택('24.6월) 에 따라 '25년 3월 업데이트 버전을 발표
- 표준 계약 조항은 고위험 AI에 대해서는 엄격한 위험관리와 책무성을, 비고위험 AI에 대해서는 행정 부담을 최소화하면서 투명성을 확보하는 이원적 구조의 계약 템플릿 제시

※ 고위험 템플릿(MCC AI High Risk) : AI 시스템의 위험·품질 관리, 데이터 거버넌스, 투명성, 정확성·견고성·사이버보안 등 「AI법」 제3장의 고위험 AI 요건을 계약 조항으로 구체화하며, 설계단계부터 사후 관리까지 공급업체의 책임 규정

※ 非고위험 템플릿(MCC AI Light) : 고위험으로 분류되지 않으나 건강·안전·기본권에 위험을 초래할 수 있는 AI 시스템에 적용하는 간소화 버전으로, 투명성, 위험관리, 데이터 거버넌스 등 핵심 관리 항목 규정

- 표준계약조항은 기존 계약에 부속서(annex)로 첨부하는 방식으로 설계되었으며, 법적 구속력은 없으나 채택 시 계약상 의무로 기능

자료명	공공행정 발전 및 혁신을 위한 생성형 AI 조달·활용 지침 行政の進化と革新のための生成 AI の調達·利活用に係るガイドライン[19]				
국가/기관	일본	자료 유형	지침·가이드라인	발표 일자	2025. 5. 27.

● 일본 디지털청(デジタル庁)은 경제산업성 및 총무성 등과 협력하여 '25년 5월 생성형 AI 활용을 촉진하고 공공 조달을 확대하기 위해 '생성형 AI 조달 활용·지침' 발표

- 조달 단계에서 공공부문은 인간중심·투명성·안전 등 'AI 사업자 가이드라인(AI事業者ガイドライン)'의 원칙에 기반하여 조달을 실행해야 하며, 데이터 취급 방침, 산출물 품질, 리스크 관리 역량 등을 점검하는 조달·계약 체크리스트를 활용하여 조달의 일관성 및 품질을 확보할 것을 요구
- 각 부처에 최고AI책임자(Chief AI Officer; CAIO)를 지정하여 AI 조달·활용에 관한 의사결정 및 책임 체계를 일원화하며, 위험 발생 시 CAIO에게 보고하고 대응하도록 규정

자료명	자동화된 의사결정에 관한 지침 개정 Directive on Automated Decision-Making[20]				
국가/기관	캐나다	자료 유형	지침·가이드라인	발표 일자	2025. 6. 24.

● 캐나다 정부는 '25년 6월 공공부문의 자동화된 의사결정에 관한 지침과 동 지침의 필수 이행 도구인 알고리즘 영향평가(Algorithmic Impact Assessment; AIA)를 개정하여 공공 AI 활용에 적용

- '자동화된 의사결정에 관한 지침'은 공공부문이 AI 등 자동화 시스템을 활용하여 의사결정 시 투명성·책임성·공정성 확보를 요구하는 정책('19년 발효)으로, '25년 6월 AIA 사전 공개 의무화, 편향 테스트 및 데이터 거버넌스 강화, 포용성 관련 조치 신설 등을 중심으로 개정
- 동 지침에 따라 캐나다 공공부문은 AI 도입 전 AIA로 영향 수준을 평가하고, 사전 자격제를 통해 검증된 공급자 풀에서 AI를 조달하는 방식으로 AI 조달 체계 운영[21]

자료명	공공부문 AI 표준 계약 조항 AI Model Clauses(v2.0)[22] AI 조달 가이드 Guidance on AI Procurement in Government[23]				
국가/기관	호주	자료 유형	지침·가이드라인	발표 일자	2025. 3. 17 / 12. 2

● 호주 디지털전환청(Digital Transformation Agency; DTA)은 공공부문의 AI 조달 전 과정을 지원하기 위해 'AI 표준 계약 조항' 및 'AI 조달 가이드' 개발

- AI 표준 계약 조항(v2.0)은 AI 제품·서비스 공급업체와 정부 기관 간 권리·의무를 규율하는 계약 조항으로, 호주 AI 윤리 원칙 및 프라이버시·사이버보안·지식재산권 등 관련 규제와 연계하여 설계되었으며, 기관별 사례에 맞춰 선택적으로 적용할 수 있는 모듈형 구조로 구성
- AI 조달 가이드는 조달 생애주기(기획-조달-관리)의 각 단계에 AI 특유의 위험과 고려 사항을 반영한 단계별 실무 지침으로, 명확한 목표 수립, 관련 법·정책 검토, 다학제 팀 구성, 데이터·인프라 준비 상태 점검 등을 포함한 조달 체크리스트 제공

□ 참고문헌

1) Tillipman, J. (2026, 3, 10). Military AI policy by contract: The limits of procurement as governance. Lawfare.
Kelley, A. (2026, 4, 1). Vendors struggle to navigate the Anthropic ban's fallout. NEXTGOV/FCW.
Dalton, M., & Thielman, N. (2026, 3, 2). Anthropic, the Pentagon, and the AI innovation ecosystem. RSTREET.
2) Executive Order 13960, Promoting the use of trustworthy artificial intelligence in the federal government. (2020, 12, 3). Federal Register.
3) AI in Government Act of 2020. H.R.2575. 116th Congress. (2020).
4) AI Training Act. S.2551. 117th Congress. (2022).
5) Advancing American AI Act. S.1353. 117th Congress. (2022).
6) Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. (2023, 10, 30). Federal Register.
7) M-24-10 Advancing governance, innovation, and risk management for agency use of artificial intelligence. (2024, 3, 28). Office of Management and Budget.
8) GSA releases generative AI acquisition resource guide for federal buyers. (2024, 4, 29). U.S. General Services Administration.
9) M-24-18 Advancing the responsible acquisition of artificial intelligence in government. (2024, 9, 24). Office of Management and Budget.
10) Executive Order 14179, Removing barriers to American leadership in artificial intelligence. (2025, 1, 31). Federal Register.
11) M-25-21 Accelerating federal use of AI through innovation, governance, and public trust. (2025, 4, 3). Office of Management and Budget.
12) M-25-22 Driving efficient acquisition of artificial intelligence in government. (2025, 4, 3). Office of Management and Budget.
13) Winning the race: America's action plan. (2025, 7, 23).
14) Executive Order 14319, Preventing woke AI in the federal government. (2025, 7, 23). Federal Register.
15) M-26-04 Increasing public trust in artificial intelligence through unbiased AI principles. (2025, 12, 11). Office of Management and Budget.
16) GSAR 552.239-7001 Basic safeguarding of artificial intelligence systems (FEB 2026) (GSAR Deviation). U.S. General Services Administration.
17) Government Digital Service. (2025, 2, 10). Artificial Intelligence Playbook for the UK

Government.
18) Updated EU AI model contractual clauses. (2025, 3, 5). European Commission.
19) 行政の進化と革新のための生成 AI の調達·利活用に係るガイドライン. (2025, 5, 27). デジタル庁.
20) Treasury Board of Canada Secretariat. (2025, 6, 24). Directive on Automated Decision-Making. Government of Canada.
21) Treasury Board of Canada Secretariat. (2026, 3, 31). Responsible use of artificial intelligence in government. Government of Canada.
22) Digital Transformation Agency. (n.d.). Contract templates. BuyICT.
23) Digital Transformation Agency. (n.d.). Guidance on AI Procurement in Government. BuyICT.

The LENS

The LENS는 주요국의 AI·디지털 정책 동향을 체계적으로 조사하고, 정기적 업데이트를 통해 정책 변화의 흐름을 지속적으로 추적·평가하는 정책 모니터링 보고서입니다.

| 작 성 |

- 한국지능정보사회진흥원 인공지능정책실 미래전략팀

  오 연 주 수석연구원 (053-230-1295, oyeonj@nia.or.kr)

| 기 획 |

- 한국지능정보사회진흥원 인공지능정책실

  이 용 진 실장　　정 지 선 팀장

  오 연 주 수석연구원

1. 본 보고서는 방송통신발전기금으로 수행한 과학기술정보통신부 정보통신·방송 연구개발사업(ICT진흥 및 혁신기반조성(정보화, R&D)사업)의 연구결과입니다.